10.18686/aitr.v2i3.4404

Application of Firewall Technology in Computer Network Information Security

Mengqiao Zhang, Peng Zhang, Xiaomei Tang

Beijing Union University, Beijing 100101

Abstract: Firewall technology is a crucial means of protection for computer network security. It achieves multi-layer protection through techniques such as packet filtering, stateful inspection, proxy technology, NAT, and VPN. Optimizing firewall technology, including multi-layer defense, dynamic rule updates, intelligent log analysis, virtualized firewall applications, and regular security assessments, can effectively enhance network security.

Keywords: Firewall; Computer; Network Information Security

1. Introduction

With the rapid development of the Internet, network security threats are increasing. As a key component of network security, the importance of firewall technology is self-evident [1]. This paper will discuss the principles, types, and applications of firewall technology in network security and propose various methods to optimize firewall technology to improve overall network protection capabilities.

2. Overview and Principles of Firewall Technology

2.1 Overview of Firewall Technology

Firewall technology is a widely used information security protection method in computer networks. As the first line of defense in a network, its main task is to monitor and control the data traffic entering and leaving the network. By analyzing data packets, firewalls can effectively prevent unauthorized access and potential network attacks, ensuring the security and stability of the internal network [2].

The earliest firewall technology dates back to the 1980s, when it was primarily used for the boundary security of corporate networks. With the rapid development of the Internet and the continuous escalation of network threats, firewall technology has also been evolving. From the initial simple packet filtering to the current deep packet inspection and advanced threat defense, firewalls have become an indispensable part of network security.

A firewall is not just a hardware device or a software tool; it represents a network security concept. By establishing strict security policies and rules, firewalls can effectively manage and control network access, protecting internal network resources from external threats. At the same time, with the rise of new technologies such as cloud computing and the Internet of Things (IoT), firewall technology continues to expand its application scope and functions to meet the security needs of different industries and scenarios.

2.2 Types of Firewalls

Firewalls can be classified into several types based on their working principles and application scenarios. The following are some common types of firewalls.

2.2.1 Network-Level Firewall

Network-level firewalls are the earliest type of firewalls. They primarily operate at the third layer of the OSI model, the network layer, by inspecting and filtering information such as the source address, destination address, and port number of IP packets to decide whether to allow the packet through. Network-level firewalls are fast and efficient, but since they only inspect the header information of packets, they are less effective at defending against application layer attacks.

2.2.2 Circuit-Level Gateway

Circuit-level gateways operate at the fourth layer of the OSI model, the transport layer. They manage the transmission of data packets by establishing and monitoring TCP or UDP connections. Circuit-level gateways can filter packets and control the establishment and termination of sessions. Although this type of firewall provides higher security than network-level firewalls, it also has a relatively greater impact on network performance.

2.2.3 Application-Level Gateway

Application-level gateways, also known as proxy firewalls, operate at the seventh layer of the OSI model, the application layer. They comprehensively inspect and filter application layer protocols through proxy mechanisms, effectively defending against various application layer attacks. Application-level gateways can deeply analyze the content of data packets and monitor and control the behavior of specific applications, providing the highest level of security protection. However, due to the need to process a large amount of data, application-level gateways typically have higher system overhead and latency.

3. Application of Firewall Technology in Computer Network Security

3.1 Application of Packet Filtering Technology in Computer Network Security

Packet filtering technology is a basic and widely used firewall technology. It inspects information such as the source address, destination address, and port number of data packets and decides whether to allow the packet through based on predefined security rules. Packet filtering technology is simple to operate, efficient, and suitable for network environments with high real-time requirements. In practical applications, packet filtering technology is primarily used to control network access, preventing unauthorized users or data packets from entering the internal network. For example, enterprises can set firewall rules to block access from specific IP addresses or allow traffic only on specific ports (such as port 80 and port 443, used for HTTP and HTTPS) to reduce the risk of network attacks [3].

Packet filtering technology can also be used to block common network attacks such as IP spoofing and port scanning. By strictly inspecting the header information of data packets, firewalls can effectively identify and block these malicious activities, protecting the network from attacks. Additionally, this technology provides enterprises with flexible access control strategies, ensuring more effective utilization of network resources.

3.2 Application of Stateful Inspection Technology in Computer Network Security

Stateful inspection technology, also known as Stateful Packet Inspection (SPI), is a more advanced firewall technology. Unlike traditional packet filtering technology, stateful inspection not only inspects the header information of data packets but also tracks the state of each packet, recording and analyzing the context of the entire communication session. This technology can dynamically identify and filter abnormal packets, thereby improving network security. For example, in a TCP connection, a stateful inspection firewall tracks the entire process of connection establishment, data transmission, and termination, ensuring that each packet is legitimate and expected. If an unexpected packet is detected, the firewall immediately blocks it.

Stateful inspection technology is widely used to defend against various complex network attacks such as SYN flood attacks and DDoS attacks. By monitoring the state of data packets in real-time, firewalls can quickly identify and respond to abnormal traffic, effectively mitigating or even preventing the impact of attacks. Additionally, this technology can enhance the reliability and stability of network communication, ensuring that legitimate packets are transmitted smoothly.

3.3 Application of Proxy Technology in Computer Network Security

Proxy technology, as an application-level gateway technology of firewalls, acts as an intermediary between the client and the server to achieve comprehensive control and filtering of data flows. Proxy firewalls can deeply analyze application layer protocols such as HTTP, FTP, and SMTP, providing more detailed and robust security protection.

Proxy firewalls not only block unauthorized access but also audit and record user behavior. For example, enterprises can use proxy firewalls to control employees' internet usage, blocking access to certain unsafe or inappropriate websites, thereby reducing security risks. Additionally, proxy firewalls can cache frequently used data, improving network access speed and efficiency.

Proxy technology is also excellent at defending against specific application layer attacks. For example, for web application attacks such as SQL injection and cross-site scripting, proxy firewalls can identify and block these malicious requests through deep packet inspection and protocol analysis, protecting the security of servers and databases.

3.4 Application of NAT and VPN Technologies in Computer Network Security

Network Address Translation (NAT) and Virtual Private Network (VPN) are two common technologies used in firewalls that play important roles in protecting computer network security.

NAT technology enhances network security by converting internal network addresses to external network addresses, thereby hiding the internal network structure and devices. Through NAT, external attackers cannot directly access internal network devices, effectively reducing the risk of network attacks. Additionally, NAT can save IP addresses and improve the utilization of network resources, making it a standard technology for most enterprise and home networks.

VPN technology establishes encrypted channels over public networks to achieve secure remote access. Enterprises can use VPN technol-

ogy to ensure that remote employees or branch offices can securely access internal network resources. By encrypting data transmission, VPN technology effectively prevents data from being intercepted or tampered with, ensuring the confidentiality and integrity of communication.

NAT and VPN technologies are often used together to build a multi-layered network security protection system. NAT hides the internal network structure, reducing the likelihood of direct attacks, while VPN provides secure remote access channels, ensuring the safety of data transmission. This combined application not only enhances the security and stability of the network but also meets the modern enterprise's needs for remote work and distributed networks.

4. Heuristic Methods for Optimizing Firewalls in Computer Network Security Prevention and Control

Firewalls play a crucial role in computer network security protection. However, as network attack methods continuously evolve, relying solely on traditional firewall technology is no longer sufficient to meet the needs of modern network security. Therefore, optimizing and enhancing firewall technology in practical applications is of paramount importance [4].

4.1 Implementation of Multi-Layer Defense Strategy

A single firewall technology is insufficient to cope with the complex and variable network attacks. Adopting a multi-layer defense strategy is an important means to enhance network security. By combining various technologies such as network-level firewalls, circuit-level gateways, and application-level gateways, a comprehensive security protection system can be formed, significantly improving overall network security[5]. For example, network-level firewalls can be deployed at the network boundary to block most external attacks; application-level gateways can be deployed within the internal network to meticulously analyze and filter application layer traffic; simultaneously, circuit-level gateways can monitor and manage the sessions at the transport layer, ensuring seamless connection of security protection at all levels.

4.2 Dynamic Rule Updates Based on Behavior Analysis

Traditional firewall rules are usually static and cannot effectively address rapidly changing network threats. The dynamic rule update method based on behavior analysis can continuously monitor and analyze network traffic, identify abnormal behaviors in real-time, and automatically adjust firewall rules to provide more flexible and efficient security protection. This method relies on big data and artificial intelligence technology[6]. Through deep learning of network traffic and analysis of behavior patterns, it can detect potential threats and attack behaviors and respond quickly. For example, when abnormal traffic patterns or access requests are detected, the system can automatically generate new firewall rules to immediately block these threats, ensuring real-time network security.

5. Conclusion

By optimizing firewall technology and constructing a multi-layered network security protection system, it is possible to effectively respond to the continuously evolving network threats, ensuring the security and stability of computer networks.

References

[1] Jiang Ke. Application and Research of firewall Technology in computer network information security [J]. Computer Optical Disc Software and Application, 2013, 16(4):178-179.(in Chinese)

[2] YAN Wuyue. Application research of Firewall Technology in Computer network Information security [J]. Computer Optical Disc Software and Application, 2013, 16(3):100-100+102.(in Chinese)

[3] Guan Zhicong, Diao Weiping. Application of Firewall technology in Computer network information security [J]. Wireless Internet Technology, 2022, 19(10):22-24.(in Chinese)

[4] ZHENG H Y. Research on Firewall technology in Computer network information security [J]. Mobile Information, 2019, 46(5):186-188. (in Chinese)

[5] Pundkar S G, Bamnote G R. Analysis of firewall technology in computer network security[J]. International Journal of Computer Science and Mobile Computing (IJCSMC), 2014, 3(4): 841-846.

[6] Wang P. Research on firewall technology and its application in computer network security strategy[J]. Frontiers in Computing and Intelligent Systems, 2022, 2(2): 42-46.